San Francisco Bay Area Grassroots Roundtable on Cyber Security

February 23-24, 2010
Westin San Francisco Airport

February 22nd

18:30 – 20:00 Onsite registration

February 23rd

Setting Research Goals and Priorities (Cypress Room)

08:00 – 08:50 Continental breakfast

08:50 – 09:00 Welcome, Overview of Goals and Outcomes - Deb Frincke, Celeste Matarazzo, Sean Peisert, Ed Talbot

09:00 – 09:10 Group exchange of desired outcomes and goals

09:10 – 10:10 **State of the Internet - Reality versus what you believe** - Richard Perlotto

10:10 – 10:30 Discussion: 1) What can this community provide that would help? 2) How can this community benefit? and 3) How is it relevant to Department of Energy (DOE)?

10:30 – 10:40 Break

10:40 – 11:40 **Unconditional Security from Noisy Quantum Storage** – Stephanie Wehner

11:40 – Noon Discussion: Three questions

Noon – 12:15 Break – gather lunch

12:15 – 13:15 **The DETER Project – Scientific, Safe and Simple CyberSecurity Experimentation** - Jelena Mirkovic

13:15 – 13:35 Discussion: Three questions

13:35 – 13:45 Break

13:45 – 14:30 Talaris Report Review – Deb Frincke and Julia Narvaez

14:30 – 16:30 Breakout Sessions – Charter to the breakout groups (2nd Floor breakout rooms)

- Analytics (Richard Strelitz)
- Emerging Technologies and Trends (Matthew Grace)
- Scientific Evaluation (Jackson Mayo)

LLNL-MI-424262

Lawrence Livermore National Laboratory
Science in the National Interest

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Sandia National Laboratories

UCDAVIS UNIVERSITY OF CALIFORNIA

16:30 – 17:30 Group summary/discussion for the first day (20 minutes each group)

18:00 – 19:30 Dinner (no host)

LLNL-MI-424262

San Francisco Bay Area Grassroots Roundtable on Cyber Security

February 23-24, 2010
Westin Hotel at San Francisco Airport

Day Two - February 24th

Identifying Opportunities (Cypress Room)

08:00 – 08:30	Working breakfast, informal discussions
08:30 – 09:00	Welcome to Day Two and summarize Day One
09:00 – 10:00	**Spamalytics: An Empirical Analysis of Spam Marketing Conversion** - Christian Kreibich
10:00 – 10:30	Discussion: Three questions
10:00 – 11:30	Breakout Group Discussions – finalize outcomes (3 groups)
	- Analytics (Richard Strelitz)
	- Emerging Technologies and Trends (Matthew Grace)
	- Scientific Evaluation (Jackson Mayo)
11:30 – 12:30	Group summary and discussion (20 minutes each group)
12:30 – 13:30	Lunch and Discussion of Opportunities, Upcoming Events and Action Items
14:00	ADJOURN

LLNL-MI-424262

Presentations

Presentation Opportunities	Theme	Candidate Presentations
Presentation 1	Analytics	1) NVAC/DHS at PNNL – Speaker TBD (Frincke) (???) 2) State of the Internet - Reality verses what you believe - Richard Perlotto
Presentation 2	Emerging Technologies and Trends	1) Unconditional Security from Noisy Quantum Storage – Stephanie Wehner 2) National Laboratory Panel (???)
Presentation 3	Scientific Evaluation	1) The DETER Project – Scientific, Safe and Simple CyberSecurity Experimentation - Jelena Mirkovic
Presentation 4	Analytics	3) Spamalytics: An Empirical Analysis of Spam Marketing Conversion - Christian Kreibich

Session Staff

Topic	Co-leads	Student Recorders	Comments
Analytics	Richard Strelitz, LANL		
Emerging Technologies and Trends	Matthew Grace, SNL		
Scientific Evaluation	Jackson Mayo, SNL		

LLNL-MI-424262

Round Table Staff

Name	Role	Email	Phone Numbers
Matt Bishop	UC Davis	bishop@cs.ucdavis.edu	(530) 752-8060 (O)
Deb Frincke	PNNL	deborah.frincke@pnl.gov	(208) 991 4DEB (G) (208) 310-1152 (C) (509) 375-3969 (O)
Celeste Matarazzo	LLNL	matarazzo1@llnl.gov	(925) 423-9838 (O) (925) 784-8253 (C)
Sean Peisert	UC Davis and LBNL	peisert@cs.ucdavis.edu	(530) 746-8717 (G)
Ed Talbot	SNL	ebtalbo@sandia.gov	(925) 294-2669 (O) (925) 784-1223 (C)
Debbie Lofrisco	LLNL	lofisco1@llnl.gov	(925) 422-0433 (O)

Titles and Abstracts

Speaker	Title	Abstract
Richard Perlotto The Shadowserver Foundation	State of the Internet - Reality verses what you believe	The Shadowserver Foundation, a non-profit organization, collects information on malicious activity and shares that gathered data freely to the appropriate network owners. This presentation will review what the current state of the Internet is, and how that effects you. Using primarily Conficker and it's wide-spread infections as

LLNL-MI-424262

		examples, we can get a better idea of what the future holds for us when looking at our network and computer security as well as the impact on all future work related to the Internet.
Dr. Stephanie Wehner Institute for Quantum Information California Institute for Technology (Caltech)	Unconditional Security from Noisy Quantum Storage	We consider the implementation of two-party cryptographic primitives based on the sole physical assumption that no large-scale reliable quantum storage is available to the cheating party. An important example of such a task is secure identification. Here, Alice wants to identify herself to Bob (possibly an ATM machine) without revealing her password. More generally, Alice and Bob wish to solve problems where Alice holds an input x (e.g. her password), and Bob holds an input y (e.g. the password an honest Alice should possess), and they want to obtain the value of some function f(x,y) (e.g. the equality function). Security means that the legitimate users should not learn anything beyond this specification. That is, Alice should not learn anything about y and Bob should not learn anything about x, other than what they may be able to infer from the value of f(x,y). We show that any such problem can be solved securely in the noisy-storage model, where we prove security against the most general attack. Our protocols can be implemented with present-day hardware used for quantum key distribution. In particular, no quantum storage is required for the honest parties.

Jelena Mirkovic, USC Information Sciences Institute	The DETER Project – Scientific, Safe and Simple CyberSecurity Experimentation	As the Internet has become pervasive and our critical infrastructures inextricably tied to information systems, the risk for economic, social, and physical disruption due to the insecurities of information systems has increased immeasurably. Over the past 10 years there has been increased investment in research on cyber security technologies by U.S. government agencies and industry. However, a large-scale deployment of effective security technology is lacking. One important reason for this deficiency is the lack of an experimental infrastructure and rigorous scientific methodologies for development and testing next-generation cyber security technologies. To address these shortcomings, the DETER project is creating the necessary infrastructure - testbeds, tools, and supporting processes - for national-scale experimentation on emerging security research and advanced development technologies for cyber defense. The DETER testbed, funded by the US Department of Homeland Security and >the National Science Foundation has been operational since 2004. Today it hosts 400+ nodes at USC/ISI and UC Berkeley, and serves more than 1,200 users and 150 projects from all over the world. It is used for academic research and teaching, and for testing commercial products. It is accompanied by a set of experimentation tools and products that make experiment setup, monitoring and control easy even at large scales. The

		DETER project has further made advances in supporting very large scale experiments via testbed federations, and in supporting safe experimentation with risky code. The next generation of the DETER project plans major improvements in experimental processes to guarantee experimental validity, >repeatability and portability. It further plans improvements in operations to support an order of magnitude larger experiments than today. Finally, it plans to build effective community tools for exchange of code, data and ideas between its users which fosters closer collaborations. This talk will describe the current state of the DETER testbed, and our new efforts aimed at advancing the science of cyber security experimentation.
Christian Kreibich International Computer Science Institute	Spamalytics: An Empirical Analysis of Spam Marketing Conversion	In his script for "All The President's Men", author William Goldman coined the famous adage "follow the money", giving Woodward and Bernstein crucial advice for their investigation. In the past years, the growth of the Internet has enabled a financially motivated underground marketplace that presents a case perhaps less politically motivated but surely no less thrilling, in which this classic strategy has remained almost entirely unused. In this talk I will present a study that sheds light on one component of this market, namely spam-based advertising. The "conversion rate" of spam -- the probability that an unsolicited email with ultimately elicit a "sale" -- underlies the entire spam value proposition. However, our understanding of this critical behavior is

		quite limited, and the literature lacks any quantitative study concerning its true value. I will describe a methodology for using parasitic infiltration of botnets -- large networks of infected computers responsible for the vast majority of spam observed today -- to empirically infer the delivery and conversion rates of spam campaigns. I will present an analysis of over 400 million instrumented spam emails across two campaigns and quantify the underlying processes that modulate its profits. The results provide insights into the entire spam conversion pipeline and illuminate some of the market pressures on the spammers and botmasters involved - and thus point out initial avenues for following the money in this poorly understood economy.